Guarding Against Bluetooth Attacks: Safeguarding Security Features

Ian Hagmann

School of Cybersecurity, Old Dominion University

CYSE 280 Windows System Management and Security

Professor Malik A. Gladden

April 17, 2024

Introduction

As cybersecurity becomes more prevalent in everyday life, individuals have to start thinking about the security of technologies they interact with. Be it connecting to a public Wi-Fi at a coffee shop or determining whether a message is phishing. Connecting devices on-the-fly has become much easier with mobile hotspots and Bluetooth. Most people would be suspicious if a stranger asked them to start a hotspot and let them connect or to connect their phone to a Bluetooth device. In this paper, I will discuss the security of Bluetooth and recommend some safe practices.

Overview of Bluetooth

Bluetooth is a wireless communication technology primarily used to create wireless personal area networks (WPANs). Bluetooth uses radio frequency (RF) to wirelessly transmit data over a short range. Bluetooth is used in many devices like smartphones, mice, keyboards, speakers, headphones, and more. There are really two types of Bluetooth: Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) and Bluetooth Low Energy (BLE) (Figueroa, 2019). Bluetooth Low Energy, as the name suggests, is a form of Bluetooth with a lower energy cost (Kurt et al., 2022). Bluetooth BR/EDR is older and more common and I will be referring to it as typical Bluetooth. BR/EDR devices form Piconets which are small ad hoc networks through Point-to-Point connections. BLE devices support Point-to-Point connections as well as Broadcasts and Mesh networks. This paper focuses more on BR/EDR but do note that BLE has its own concerns with security and privacy.

Bluetooth Security Features

This section describes the security mechanisms in Bluetooth technology. Bluetooth security only includes the scope of its own connection between two devices and cannot perform

end-to-end security alone (Padgette et al., 2022). There are five security services within the Bluetooth standard which include: authentication, confidentiality, authorization, message integrity, and pairing/bonding.

Pairing

Typical Bluetooth devices pair with each other when one sends out an RF signal looking for the other, whereas Bluetooth Low Energy devices advertise themselves. For encryption and authentication to take place within Bluetooth, a secret symmetric key must be generated. Typical Bluetooth devices call this key the Link Key and Low Energy devices call it the Long Term Key. There are two ways to generate link keys: Personal Identification Number (PIN)/Legacy Pairing and Secure Simple Pairing (Padgette et al., 2022). To finalize pairing, devices have to authenticate each other, which will be described in the next section.

PIN/Legacy Pairing

PIN/Legacy pairing uses a user entered PIN in one or both devices to derive link keys. The PIN can be 1 to 16 bytes of binary or if a human is involved, 4 to 8 alphanumeric characters. If the PIN is less than 16 bytes then some of the initiating device's unique address is added to pad the length. The process itself involves multiple random numbers and temporary keys. The first device generates an initial random number and sends it to the second device. Then they both take that random number and the PIN as inputs for an encryption algorithm to generate an initial key. Next both devices generate new random numbers, XOR them with the initial key, and send the result to each other. Then they XOR those results back to get each other's random number to encrypt using the other's device address to get a key. Another key is generated using their own random number and address. Then finally they XOR those two keys with each other to generate the same link key.

Secure Simple Pairing

Secure Simple Pairing (SSP) added security through the addition of public key cryptography to protect against eavesdropping and man-in-the-middle (MITM) attacks (Padgette et al., 2022). SSP is also more flexible for input and output of devices involved by offering four different association models: Numeric Comparison, Passkey Entry, Just Works, and Out of Band (OOB). For pairing, Bluetooth devices exchange public keys and encrypt them with their private keys to calculate a temporary key. Depending on the association model used, random values are exchanged. Those values are input into an encryption algorithm along with addresses and temporary keys and the results are sent to the other for comparison. If those values match, another encryption algorithm with similar inputs is used to generate the link key.

Numeric Comparison.

Numeric Comparison can be used when both Bluetooth devices can display a 6 digit number and a user can input “yes” or “no” in some way. Both devices would show the user a 6 digit number during pairing and the user can determine whether pairing should succeed or fail. One thing to note is that the shown 6 digit number is not used in link key generation.

Passkey Entry.

Passkey Entry can be used when one Bluetooth device has input like a keyboard and the other only has a display. A 6 digit number will be shown on the device with only a display and the user can enter it into the other device. Similarly, the 6 digit number will not be used to derive the link key.

Just Works.

Just Works is used when one device has no display or input device. Like with Numeric Comparison, both devices generate a 6 digit number but the user has to just accept the pairing without confirming.

Out of Band (OOB).

OOB can be used when the Bluetooth devices have additional communications technology for discovery and data exchange. Exact methods vary, but in the case of Near Field Communication (NFC), devices can be brought close to each other and a single button push would accept a pairing.

Authentication

Authentication is the act of verifying the identity of communicating entities. Bluetooth uses a challenge-response scheme for authentication. For the challenge-response scheme one machine sends a challenge for the other machine to alter using their secret key and respond with. If the response matches the machine's own altering of their challenge with the secret key, the machine can trust the other. Bluetooth has Legacy Authentication as well as Secure Authentication, of which Secure Authentication is preferred (Padgette et al., 2022). Legacy Authentication is a fall back in case one party doesn't support Secure Authentication. Authentications attempts that fail starts a longer and longer timer in a Bluetooth device before it'll attempt to authenticate again.

Legacy Authentication

The two devices participating in the authentication are called the claimant, the one trying to connect, and the verifier, the one authenticating the connection. First, the verifier sends a 128-bit random challenge, generated using a pseudo random number generator, to the claimant. Then

the claimant uses an encryption algorithm with their Bluetooth device address, the link key, and random challenge as inputs. At the same time the verifier performs the same encryption with the same inputs. The claimant sends the first 32 bits to the verifier as response to the challenge. Note that the other 96 bits are not included and will be used later for encryption key generation. Lastly, the verifier compares the response 32 bits to the first 32 bits of its own calculation. If they match, authentication is completed, and if they don't, authentication failed and the timer is started. This completes a one-way authentication; the Bluetooth standard allows for the roles to be reversed and process repeated to complete mutual authentication.

Secure Authentication

Like with the Legacy Authentication, I will be using claimant and verifier. First the claimant and verifier send 128-bit random challenges to each other. Then they both use a stronger hashing algorithm with both addresses, the link key, and both random challenges as inputs. Once again, the first 32 bits are sent and the other 96 are stored for later use. They send their responses to each other and compare what they computed with what was given to them as a response. If they match, authentication is completed, and if they don't, authentication failed and the timer is started. Unlike the Legacy Authentication, this completes a mutual authentication without the need for a second authentication.

Confidentiality

Confidentiality is ensuring that data is only seen by trusted entities. Bluetooth offers a confidentiality service in the form of encryption. There are three encryption modes, though only two provide confidentiality (Padgette et al., 2022). For Encryption Mode 1, no traffic is encrypted at all, Encryption Mode 2 encrypts traffic destined for one host using individual link keys for encryption keys, but not broadcasts, and Encryption Mode 3 encrypts all traffic using

the device's link key for encryption key generation. Modes 2 and 3 can use either of two stream cipher encryption algorithms. I will not go into detail on these algorithms but know that one is considered more secure than the other. The encryption key can range from 1 to 16 bytes in increments of 1 byte. The length is negotiated between two devices by going back and forth suggesting lengths until they agree. Initial suggestions are programmed in by the manufacturer and they can also specify a minimum acceptable length.

Authorization

Authorization describes the level of trust between Bluetooth devices with more trust leading to more access. Trusted devices will be given full access to services provided by the other device. Untrusted devices will have restrictions on what services they can access. Individual service security can define requirements of authentication, encryption, and authorization. For typical Bluetooth devices if encryption is required, then authorization must be as well due to a component of encryption keys coming from the authorization process. Bluetooth also allows for further defining of policies so that even in a trust relationship, access can be restricted. Authorization defined in the Bluetooth standard only authenticates devices and not users, but applications can still enforce their own securities.

Type of Threats

A threat can be defined as any action that may cause harm to systems (Hassan et al., 2018). These threats often exploit vulnerabilities in a system to accomplish something specific like injecting malicious software or disrupting communications. These vulnerabilities are flaws in the security features like authentication. In a broad sense, there are two types of threats: attacks and malware.

Attack Threats

Attacks on Bluetooth devices mainly attempt to gain unauthorized access to a victim's device or data without their knowledge (Hassan et al., 2018). Attacks often mean to disable/destroy devices or alter/steal data. These attacks may be active, meaning that a current effort is made by a person, or passive, meaning that a computer is automatically performing them. Attacks can target the victim's device or the victim themself by tricking them.

Malware Threats

Malware is the name for malicious software intending to do harm (Hassan et al., 2018). As Bluetooth is a communications technology, malware doesn't typically target Bluetooth itself. Instead, Bluetooth is simply the point of entry into a system to infect it and may be used to spread.

Known Attacks

There are many known attacks on Bluetooth, so I will only talk about a few. PIN cracking attacks involve capturing the random numbers and addresses involved in pairing and authentication (Minar & Tarique, 2012). Then brute forcing every possible PIN number in the same way that the link key is derived. Having the link key allows for the attacker to decrypt traffic. MITM attacks involve a device virtually connecting two unknowing ones by connecting to each using different Just Works link keys and forwarding messages (Minar & Tarique, 2012). This allows an attacker to not only decrypt traffic, but also compromise the integrity of messages. Denial of Service (DoS) attacks can occur in a number of ways and their intention is to stop devices from communicating (Minar & Tarique, 2012).

Countermeasures

Preventing these attacks is paramount for the continuation of Bluetooth and so much work has been done to stop them. Updates to Bluetooth firmware, software, and devices have come out to prevent certain attacks by patching the vulnerabilities they utilized (Haataja et al., 2013). Sensitive data that is transmitted should use strong encryption to prevent the capture of traffic and be transmitted using the least power to minimize the distance it travels. Trying to keep Bluetooth device addresses secret can slow attacks, but methods are available to find them in minutes (Haataja et al., 2013). To try and prevent PIN cracking, only long PINs should be used. As Bluetooth is only a communication technology, applications should have their own additional security in place. Enforcing that SSP devices do not accept Just Works link keys can prevent MITM attacks (Haataja et al., 2013). More human involvement like with a button press on every connection can help prevent unauthorized connections. Depending on the type of DoS attack, it can be impossible to stop it without physically moving to another location. Some DoS attacks can be prevented by ignoring unauthenticated transmissions.

Best Practices

As always, the first step in security is being aware of security so individuals using Bluetooth should be informed on best practices (Minar & Tarique, 2012). Choosing strong PINs that are long, random, and not unchanging between connections is important. Configuring devices to use stronger security features and establishing a minimum security level is good practice. Making it so that devices addresses aren't discoverable outside of pairing would help a little (Minar & Tarique, 2012). Turning off Bluetooth devices when they are not in use can save power and stop attacks from even beginning. Pairing should be done as infrequently as possible and in private areas. Users should not interact with unsolicited pairing messages. When a device

is lost or stolen, users should un-pair all the devices that were paired to it (Minar & Tarique, 2012).

Conclusion

Bluetooth is a communication technology present in the everyday life for many people, so we should be mindful of its security. Bluetooth is primarily used for forming ad hoc networks between two devices. The security of Bluetooth can only protect its own scope and offers five services: authentication, confidentiality, authorization, message integrity, and pairing/bonding. Most of those services offer legacy modes and newer, more secure ones. Bluetooth's security services aim to protect against attack and malware threats to system wellbeing. There are many attacks, some of which have been patched against and others require user decisions. Ensuring that devices aren't in a position to be threatened by turning them off, pairing in secure locations, or disabling discoverability are some of the best practices. Knowing that Bluetooth offers these security features is the first step in securing data. The next step is actually using them.

References

Figueroa Lorenzo, S., Añorga Benito, J., García Cardarelli, P., Alberdi Garaia, J., & Arrizabalaga Juaristi, S. (2019). A comprehensive review of RFID and Bluetooth Security: Practical Analysis. *Technologies*, *7*(1), 15. https://doi.org/10.3390/technologies7010015

Haataja, K., Hyppönen, K., Pasanen, S., & Toivanen, P. (2013). Bluetooth security attacks. *SpringerBriefs in Computer Science*. https://doi.org/10.1007/978-3-642-40646-1

Hassan, S. S., Bibon, S. D., Hossain, M. S., & Atiquzzaman, M. (2018). Security threats in bluetooth technology. *Computers & Security*, *74*, 308–322. https://doi.org/10.1016/j.cose.2017.03.008

Kurt Peker, Y., Bello, G., & Perez, A. J. (2022). On the security of Bluetooth Low Energy in two consumer wearable heart rate monitors/sensing devices. *Sensors*, *22*(3), 988. https://doi.org/10.3390/s22030988

Minar, N. B.-N. I., & Tarique, M. (2012). Bluetooth security threats and solutions: A survey. *International Journal of Distributed and Parallel Systems*, *3*(1), 127–148. https://doi.org/10.5121/ijdps.2012.3110

Padgette, J., Bahr, J., Batra, M., Holtmann, M., Smithbey, R., Chen, L., & Scarfone, K. (2022). Guide to bluetooth security. *NIST Special Publication 800-121,* (Revision 2). https://doi.org/10.6028/nist.sp.800-121r2-upd1